Zone Configuration

This chapter describes zone configuration. It includes the following major sections:

- Basic Zone Configuration
- Zone Remote Guard List
- Zone Traffic Learning
- Zone Detection

Basic Zone Configuration

This section describes the initial Zone configuration procedures that relate to zone parameters such as: zone name, description, and zone IP address.

It describes the following procedures:

- Defining a New Zone
- Duplicating a Zone
- Removing a Zone
- Removing All Zones
- Displaying Zone Templates
- Entering a Zone Command Level
- Describing a Zone
- Defining the Zone IP Address

- Removing a Zone IP Address
- Removing all Zone IP Addresses

Defining a New Zone

The Detector enables the user to define a new zone based on a variety of templates.

To define a new zone perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# zone <new-zone-name> [<template>|copy-from
   <base-zone-name>][interactive]
   ```

   Where:

   – *new-zone-name*—A zone name string. An alphanumeric string should start with a letter, hold no spaces, and should be limited to a length of up to 63 characters. The string may contain underscores.

   – *template*—(Optional) A template that defines the zone configuration. Options are:

   Default —The Guard default zone template

   Bandwidth-limited Link Templates—Templates designed and specifically tailored for detection of large subnets segmented according to zones with known bandwidth. Detection on zones defined by these templates can be assumed without undergoing the learning process. It is recommended to define such a zone with protect-ip-state of only-dest-ip (see the "Guard-Protection Activation Forms" section for further details). The following bandwidth-limited link templates are available for 128K, 1M, 4M, and 512K links respectively: **LINK_128K**, **LINK_1M**, **LINK_4M**, and **LINK_512K**.

   Note Learning Phase 1, policy construction, cannot be performed for these templates.

Note If no zone template is specified, the zone will be defined using the Detector DEFAULT zone template.

- *base-zone-name*—(Optional) The name of a desired zone used as a template for the new zone.
- **interactive**—(Optional) The operation mode of the new zone is set to interactive (see the "Interactive Recommendations Mode" section for further details).

Note Choosing **Enter** without specifying the zone template defines a zone by the Detector default zone template.

2. Choose **ENTER**. Below is an example of the **zone** command implementation:

```
admin@DETECTOR-conf# zone scannet
admin@DETECTOR-conf-zone-scannet#
```

Duplicating a Zone

The user may duplicate a desired zone and define a new, identically- configured, zone.

To duplicate a zone from the Configuration command group level perform the following:

1. From the Configuration command group level type the following:

```
admin@DETECTOR-conf# zone <new-zone-name> copy-from
<base-zone-name>
```

Where:

- *new-zone-name*—A zone name string. An alphanumeric string should start with a letter, hold no spaces, and should be limited to a length of up to 63 characters. The string may contain underscores.
- *base-zone-name*—The name of a desired zone used as a template for the new zone.

2. Choose **ENTER**. The following prompt appears:

   ```
   admin@DETECTOR-conf-zone-<new-zone-name>#
   ```

To duplicate a zone from the zone command group level perform the following:

1. From the Zone command group level of the desired zone type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># zone <new-zone-name>
   copy-from-this
   ```

   Where *new-zone-name* specifies a zone name string. An alphanumeric string should start with a letter, hold no spaces, and should be limited to a length of up to 63 characters. The string may contain underscores.

2. Choose ENTER. Below is an example of the **zone** command implementation:

   ```
   admin@DETECTOR-conf-zone-scannet# zone mailserver copy-from-this
   admin@DETECTOR-conf-zone-mailserver#
   ```

Removing a Zone

The user may remove a desired zone.

Caution Removing a zone eliminates its DDoS detection.

To remove a desired zone perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# no zone <zone-name>
   ```

   Where *zone-name* identifies the zone name. Use '*' to remove all zones.

2. Choose **ENTER**.

Note The Detector allows inserting an asterisk (*) as a wildcard character at the end of a zone name. Thus, a user may use the wildcard character (*) to remove several zones with the same prefix in one command.

Removing All Zones

The user may remove all the Detector's zones.

Caution Removing all zones eliminates their DDoS detection.

To remove all zones perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# no zone *
   ```

2. Choose **ENTER**.

Displaying Zone Templates

The Detector enables the user to display a specific zone template or all zone templates.

To display all zone templates perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# show templates
   ```

2. Choose **ENTER**. The following (sample) screen appears:

   ```
   admin@DETECTOR# show templates
    DEFAULT
    LINK_1M
    LINK_4M
    LINK_128K
    LINK_512K
   admin@DETECTOR#
   ```

To display a specific zone template perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# show templates [<template-name> [policies]]
   ```

Where:

– *template-name*—A zone template. Options include:

Default —The Guard default zone template

LINK_128K—A template designed for bandwidth-limited Links

LINK_1M—A template designed for bandwidth-limited Links

LINK_4M—A template designed for bandwidth-limited Links

LINK_512K— A template designed for bandwidth-limited Links

Note If no template name is specified, the list of zone templates is displayed.

2. Choose **ENTER**. The following sample screen appears:

```
admin@DETECTOR-conf# show templates DEFAULT
Zone is INACTIVE
Operation Mode: AUTOMATIC
Description:
Zone ID: 0
Template: DEFAULT
PROTECT IP STATE: all-zone
FLEX-FILTER:
FLEX-FILTER ACTION: disable

admin@DETECTOR-conf#
```

Entering a Zone Command Level

The user should enter a zone command level to perform zone specific operations and procedures.

To enter a zone command level perform the following:

1. From the Configuration command group level type the following:

```
admin@DETECTOR-conf# zone <zone-name>
```

Or alternatively:

From the Global command group level type the following:

```
admin@DETECTOR# configure <zone-name>
```

Where *zone-name* specifies the desired zone name.

2. Choose **ENTER**. Below is an example of the zone command implementation:

```
admin@DETECTOR-conf# zone scannet
admin@DETECTOR-conf-zone-scannet#
```

Describing a Zone

The user may add a description to a zone for identification purposes.

To add a description to a zone perform the following:

1. From the Zone command level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># description <string>
```

Where *string* specifies a string that describes the zone. The string length is limited to a maximum of 80 characters.

2. Choose **ENTER**. Below is an example of the **description** command implementation:

```
admin@DETECTOR-conf-zone-scannet# description Scannet Zone used
for demonstration purposes
admin@DETECTOR-conf-zone-scannet#
```

Note To modify a zone's description repeat the zone description procedure. The new description overrides the former.

Defining the Zone IP Address

The user must define a zone IP address to enable the Detector to perform traffic learning and detection procedures.

To define the zone IP address perform the following:

1. From the Zone command level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># ip address <ip-addr>
[<ip-mask>]
```

Where:

- *ip-addr*—The zone IP address.

– *ip-mask*—(Optional) The zone IP subnet mask.

Note If no mask is specified, the Detector assumes the default subnet mask 255.255.255.255.

2. Choose **ENTER**. Below is an example of the **ip address** command implementation:

```
admin@DETECTOR-conf-zone-scannet# ip address 192.168.100.34
admin@DETECTOR-conf-zone-scannet#
```

Note When initially defined, the zone IP address should be inserted when the zone is undetected. However, a zone's subnet IP address or its additional IP addresses may be added when the zone is in the detected mode.

Note The zone IP address procedure should repeat per each zone IP address or subnet mask.

Removing a Zone IP Address

The user may remove a zone IP address.

Caution Removing a zone's IP address may compromise the zone's DDoS detection.

To remove a zone's IP address perform the following:

1. From the desired Zone command group level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># no ip address <ip-addr>
[<ip-mask>]
```

Where:

– *ip-addr*—The zone IP address. Use '*' to remove all zone IP addresses.

– *ip-mask*—(Optional) The zone IP subnet mask.

Note If no mask is specified, the Detector assumes the default subnet mask 255.255.255.255.

2. Choose **ENTER**. Below is an example of the **no ip** address command implementation:

```
admin@DETECTOR-conf-zone-scannet# no ip address 192.168.100.34
admin@DETECTOR-conf-zone-scannet#
```

Removing all Zone IP Addresses

The user may remove all the zone IP addresses.

Caution Removing all zone IP addresses eliminates the zone DDoS detection.

To remove all the zone's IP addresses perform the following:

1. From the desired Zone command group level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># no ip address *
```

2. Choose **ENTER**.

Zone Remote Guard List

The Detector has a list containing a Guard (or Guards) to remotely activate when a traffic abnormality is detected. The zone remote Guard list is part of the zone configuration. When the Detector detects a traffic abnormality it first consults the zone remote Guard list for alerting (provided the Detector is configured for remote-activation).

If the Detector does not find a Guard on the list it refers to the remote Guard (or Guards) on the Detector default list (see the "Default Remote Guard List" section in Chapter 3, "Detector Configuration" for further details).

This section contains the following procedures:

- Adding a Guard to the Zone Remote Guard List
- Removing a Guard from the Zone Remote Guard List
- Interactive Recommendations Mode

Adding a Guard to the Zone Remote Guard List

The user may add one or more Guards to the zone remote Guard list.

To add a remote Guard or Guards to the zone remote Guard list perform the following:

1. From the Zone command group level type the following:

   admin@DETECTOR-conf-zone-<*zone-name*># **remote-guard** <*remote-guard-address*> [<*description*>]

   Where:

   - *remote-guard-address*—The desired remote Guard IP address.
   - *description*—(Optional) The remote Guard description (a maximum of 63 characters).

2. Choose **ENTER**.
3. Repeat steps one and two as many times as required.

Below is an example of the **remote-guard** command implementation:

```
admin@DETECTOR-conf-zone-scannet# remote-guard 192.168.100.33
admin@DETECTOR-conf-zone-scannet#
```

Removing a Guard from the Zone Remote Guard List

The user may remove a Guard from the remote Guard list.

To remove a Guard from the remote Guard list perform the following:

1. From the Zone command group level type the following:

   admin@DETECTOR-conf-zone-<*zone-name*># **no remote-guard** <*remote-guard-address*>

Where *remote-guard-address* specifies the remote Guard IP address. Use '*' to remove all remote Guards from the remote Guard list.

Caution The user should verify that the Detector has at least one remote Guard on its default remote Guard list (see the "Default Remote Guard List" section in Chapter 3, "Detector Configuration" for further details).

2. Choose **ENTER**.
3. Repeat steps one and two as many times as required.

Below is an example of the **no remote-guard** command implementation:

```
admin@DETECTOR-conf-zone-scannet# no remote-guard 192.168.100.33
admin@DETECTOR-conf-zone-scannet#
```

Interactive Recommendations Mode

In the Interactive Recommendation mode the Detector enables the user to decide on the activation of the filters the policies launch (see the "Interactive Recommendations Mode" section in Chapter 6, "Filter Procedures"for details). The Detector functions in accordance with the user's decision to accept, ignore, or time the filter's activation. In this way the Detector lets the user decide on the production of its detection measures in real time.

Activating the Interactive Recommendation Mode

The user may activate the interactive recommendations mode for any desired zone and continue to apply the procedure over a number of zones. The user may activate the interactive mode when a zone is defined, or later, either before or after initiating zone detection. The Detector enables the user to apply the interactive recommendations mode from the Configuration or from the desired zone's command group levels.

To activate the interactive recommendation mode perform the following:

1. From the Zone command group level type the following (sample):

   ```
   admin@DETECTOR-conf-zone-<zone-name># interactive
   ```

2. Choose **ENTER**.

To create a new zone with interactive recommendations mode perform the following:

1. From the Configuration command group level type the following:

   ```
   admin@DETECTOR-conf# zone <new-zone-name> interactive
   ```

2. Choose **ENTER**.

The new zone is created with a DEFAULT zone template configured for interactive recommendations mode. See the "Defining a New Zone" section for further details.

Deactivating the Interactive Recommendation Mode

The user may deactivate the interactive recommendations mode for any desired zone or zones at any time. Deactivating this mode results in the Detector disregarding any recommendations and assuming an automatic detection functioning such as automatically producing dynamic filters, etc. The user may deactivate the interactive recommendations mode from the desired zone's command group level.

To deactivate the interactive recommendation mode perform the following:

1. Type the following (sample):

   ```
   admin@DETECTOR-conf-zone-<zone-name># no interactive
   ```

2. Choose **ENTER**.

Zone Traffic Learning

As the user initializes the Learning phase (see the "Learning Phase 1 – Policy Construction" section in this chapter), the Detector learns the zone's (zones') traffic characteristics. The results of this stage will be translated into detection policies. The Learning system constructs the Detector detection policies that instruct the Detector detection system as for how to regard the zone traffic flows.

Note For the learning phases to take place port mirroring must be configured on the switch or the Detector must be connected to a router using an optical splitter.

The Detector's tools for constructing detection policies are the Policy Templates. These define the policies according to the Minimum Threshold and Maximum Services parameters the user provides (this chapter will not cover those advanced procedures see Chapter 7, "Policy Procedures" for further details).

Once supplied with the appropriate parameters, the Detector's Policy Templates construct the detection policies based on the zone traffic and tune the constructed policies based on the learned thresholds. The user is called to approve (accept) or reject each one of the learning phases. The learning is performed for each of the Detector zones (if applicable).

The Learning phase consists of the following:

- **Learning Phase 1–Policy Construction**—This is the phase in which the Detector constructs its policies with its user-defined or self-configured Policy Templates. This phase consists of traffic flowing transparently through the Detector, enabling it to discover which services are used by the zone. This chapter will detail a procedure based on the Detector's Minimum Threshold and Maximum Services default parameters (see Chapter 7, "Policy Procedures" for further details).
- **Learning Phase 2 –Threshold Tuning**—This is the phase in which the Detector tunes its detection policies thresholds to closely adapt to zone traffic (see Chapter 7, "Policy Procedures" for further details).

Learning Phase 1 – Policy Construction

Note The user is directed through the Detector Learning phases without parameter definitions. For the Learning phases' parameter definitions refer to Chapter 7, "Policy Procedures".

To begin the first Learning phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# learning policy-construction <zone-name>
   ```

   Or alternatively:

   From the zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># learning policy-construction
   ```

Where *zone-name* specifies a zone name.

Note that the Guard enables the use of an asterisk (*) as a wildcard denoting either of the following options:

- All of the Guard's zones. Issuing **learning policy-construction*** means setting the policy construction phase for all of the Detector's zones.
- A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Note Cisco recommends letting the Learning Phase 1 - Policy Construction continue for at least two hours prior to proceeding to the next phase.

Note Policy Construction cannot be performed for zones based on the bandwidth-limited link templates: LINK_128K, LINK_1M, LINK_4M, LINK_512K.

Terminating Learning Phase 1 –Policy Construction

After a sufficient period of time (see the above note) the user ends the Policy Construction phase. The user may accept the Detector's suggested policies.

The user may decide to abort the first phase of the Learning process. In this case, the Detector stops the process and erases all its learned data. As a result, the Detector falls back into its default settings (in the case of a new zone) or to the zone traffic configurations it had prior to the initiation of the learning process.

The user may decide to view the learning process outcomes prior to making a decision. See the "Zone and Learning Phase Snapshot" section in Chapter 7, "Policy Procedures" for further details.

Accepting Learning Phase 1 – Policy Construction

The user may accept the Detector's suggested policies.

To accept the results of the initial Policy Construction phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# no learning <zone-name> accept
   ```

   Or alternatively:

   From the Zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># no learning accept
   ```

   Where *zone-name* specifies a zone name.

   Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

   - All of the Detector's zones. Issuing **no learning* accept** means ending and accepting the learning results for all of the Detector's zones.
   - A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Aborting Learning Phase 1 – Policy Construction

The user may decide to abort the first phase of the Learning procedure. In this case the Detector stops the process, erases all its learned data, and reverts back its default settings (in the case of a new-zone) to the zone traffic configurations it had prior to the aborted Learning phase.

To abort the Policy Construction phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# no learning <zone-name> reject
   ```

   Or alternatively:

   From the Zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># no learning reject
   ```

   Where *zone-name* specifies a zone name.

Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

- All of the Detector's zones. Issuing **no learning* reject** means aborting the learning phase for all of the Detector's zones.
- A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Learning Phase 2 – Threshold Tuning

During this stage the Detector constructs its detection policies and begins to tune its traffic type thresholds (see Chapter 7, "Policy Procedures" for further details).

To begin the second Learning phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# learning threshold-tuning <zone-name>
   ```

   Or alternatively:

   From the zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># learning threshold-tuning
   ```

   Where *zone-name* specifies a zone name.

   Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

   - All of the Detector's zones. Issuing **learning threshold-tuning*** means setting the threshold tuning phase for all of the Detector's zones.
   - A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Note Cisco Systems recommends letting the Learning Phase 2 - Threshold Tuning continue for 24 hours before concluding.

Terminating Learning Phase 2 – Threshold Tuning

After a sufficient period of time (see the above note) the user ends the Threshold Tuning phase. The user may accept the Detector's suggested policies or decide to abort the second phase of the learning process. The Detector would stop the Threshold Tuning phase and adopt the Policy Construction Phase results and the former thresholds results the Detector has. This results in a situation in which newly constructed policies have thresholds that were obtained according to past traffic characteristics.

The user may decide to view the learning process outcomes prior to making a decision. See the "Zone and Learning Phase Snapshot" section in Chapter 7, "Policy Procedures" for further details.

Accepting Learning Phase 2 – Threshold Tuning

The user may accept the Detector's suggested thresholds.

To accept the results of the Threshold Tuning phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# no learning <zone-name> accept
   ```

   Or alternatively:

   From the Zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># no learning accept
   ```

   Where *zone-name* specifies a zone name.

   Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

   - All of the Detector's zones. Issuing no **learning* accept** means ending and accepting the learning results for all of the Detector's zones.
   - A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

The Detector is now tuned to the zone traffic characteristics and ready to detect the zone (a procedure launched by issuing the **detect** command).

Aborting Learning Phase 2 – Tuning Threshold

The user may wish to abort the second phase of learning procedure. In this case the Detector stops the process and erases the data learned on the second phase. The data gathered on the first learning phase and on the previous learning phase 2 remain unchanged. This results in a situation in which newly constructed policies have thresholds that were obtained according to past traffic characteristics.

To abort the second Learning phase perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# no learning <zone-name> reject
   ```

   Or alternatively:

   From the Global command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># no learning reject
   ```

   Where *zone-name* specifies a zone name.

   Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

   - All of the Detector's zones. Issuing **no learning* reject** means aborting the learning phase for all of the Detector's zones.
   - A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Learning Phase Verification

The user may wish to verify whether the Detector has undergone its learning phase (with its detection policies functioning properly) has succeeded. The indication would be a display of the policies functioning properly.

The user launches the **detect** command see the "Zone Detection" section for further details.

To verify the status of the learning phase perform the following:

1. From the Zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># show policy statistics
   ```

2. Choose **ENTER**. The following (partial sample) screen appears:

```
admin@DETECTOR-conf-zone-scannet# show policies statistics
Key              Rate         Policy
192.168.100.34   73.17        http/80/analysis/syns/dst_ip
N/A              0.17         http/80/analysis/syns/global

Key              Ratio        Policy
192.168.100.34   1.44
tcp_ratio/any/analysis/syn_by_fin/dst_ip_ratio
80               1.44
tcp_ratio/any/analysis/syn_by_fin/dst_port_ratio

Key              Connections  Policy
N/A              429.00
tcp_connections/any/analysis/in_nodata_conns/global
```

The sample screen displays that the detector policies are receiving traffic and functioning properly.

Zone Detection

After learning the zone traffic characteristics the Detector is ready for zone detection. The user may wish to command the Detector to detect right after completing the zone configurations. The Detector would then begin applying its detection policies.

To detect the zone perform the following:

1. From the Global command group level type the following:

   ```
   admin@DETECTOR# detect <zone-name>
   ```

   Or alternatively:

   From the Zone command group level type the following:

   ```
   admin@DETECTOR-conf-zone-<zone-name># detect
   ```

   Where *zone-name* specifies a zone name.

Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

- All of the Detector's zones. Issuing **detect *** means beginning detection for all of the Detector's zones.
- A wildcard denoting zone names (i.e. OBL*).

2. Choose **ENTER**.

Guard-Protection Activation Forms

The Detector enables the user to apply different Guard-protection forms designed to save Guard-protection resources and better focus on the zone detection and protection requirements. Those protection forms range from assuming protection over a particular zone (i.e. a specific server) that is a part of an overall zone (i.e. a protected network environment) to assuming protection over all of the zones of the overall zone. The Detector's Guard-protection activation forms are the following:

- The Detector activates the Guard to assume protection over the overall zone whenever a traffic abnormality is detected. This strategy is recommended when the overall zone consists of intra-related zones that cannot be risked.
- The Detector activates the Guard protection over a particular zone once a traffic abnormality is traced as destined to that particular zone. This is recommended when the overall zone consists of unrelated particular zones. This is since the user may want to assume protection per an attacked zone and not spend valuable protection resources over the overall zone.
- The Detector activates the Guard protection over a specific zone once a traffic abnormality is traced as destined to that specific zone. The Detector would also activate the Guard protection over the overall zone once the detected abnormality cannot be associated with a particular zone. This strategy is recommended when the overall zone consists of highly related particular zones. This is since the user may want to avoid a situation in which a targeted zone may inflict damage on the overall zone.

To activate the Guard-protection forms perform the following:

1. From the following sample Zone command group level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># protect-ip-state {all-zone | only-dest-ip | policy-type}
```

Where:

- **all-zone**—The Detector activates the Guard to assume protection over the overall zone whenever a traffic abnormality is detected (see this section's explanation for further details).
- **only-dest-ip**—The Detector activates the Guard protection over a particular zone once a traffic abnormality can be traced as destined to that particular zone (see this section's explanation for further details).
- **policy-type**—The Detector activates the Guard protection over a particular zone once a traffic abnormality can be traced as destined to that particular zone (see this section's explanation for further details).

2. Choose ENTER.

Zone Detection Verification

The user may wish now to issue the **show counters** command to display the zone status to verify that the detection process is functioning properly.

To verify that the zone detection is functioning properly perform the following:

1. From the Zone command group level type the following:

   admin@DETECTOR-conf-zone-<*zone-name*># **show counters** [**history**]

   Where **history** displays the Received counter values for every minute in the past hour. The counter is measured in packets and in Kbits.

Note By default, only the current counter is displayed.

2. Choose **ENTER**. The following (sample) screen appears:

```
admin@DETECTOR-conf-zone-scannet# show counters history
Time                 Received(Pkts)   Received(KBits)
current              239298           1159253
Oct 23 2003 00:57:53 148744           664494
Oct 23 2003 00:56:53 148744           664494
Oct 23 2003 00:55:54 148744           664494
... ... ...
admin@DETECTOR-conf-zone-scannet#
```

The sample screen indicates that zone traffic is mirrored (or split), the Detector receives the zone's traffic and the traffic shows normal flow fluctuations. Zone detection is functioning properly.

Ending the Zone Detection

The user may wish to end the zone detection.

To end a zone's protection, from the Global command group level type the following:

```
admin@DETECTOR# no detect <zone-name>
```

Or alternatively:

From the Zone command group level type the following:

```
admin@DETECTOR-conf-zone-<zone-name># no detect
```

Where *zone-name* specifies a zone name.

Note that the Detector enables the use of an asterisk (*) as a wildcard denoting either of the following options:

- All of the Detector's zones. Issuing **no detect *** means ending detection for all of the Detector's zones.
- A wildcard denoting zone names (i.e. OBL*).

To know more about the Detector filter system, filter types, and filter configuration refer to Chapter 6, "Filter Procedures" for further details.